

# Password Policies Best Practice

Andreas Georgiou

*Supervised by:* Professor Angela M. Sasse

September 2014



# The Problem

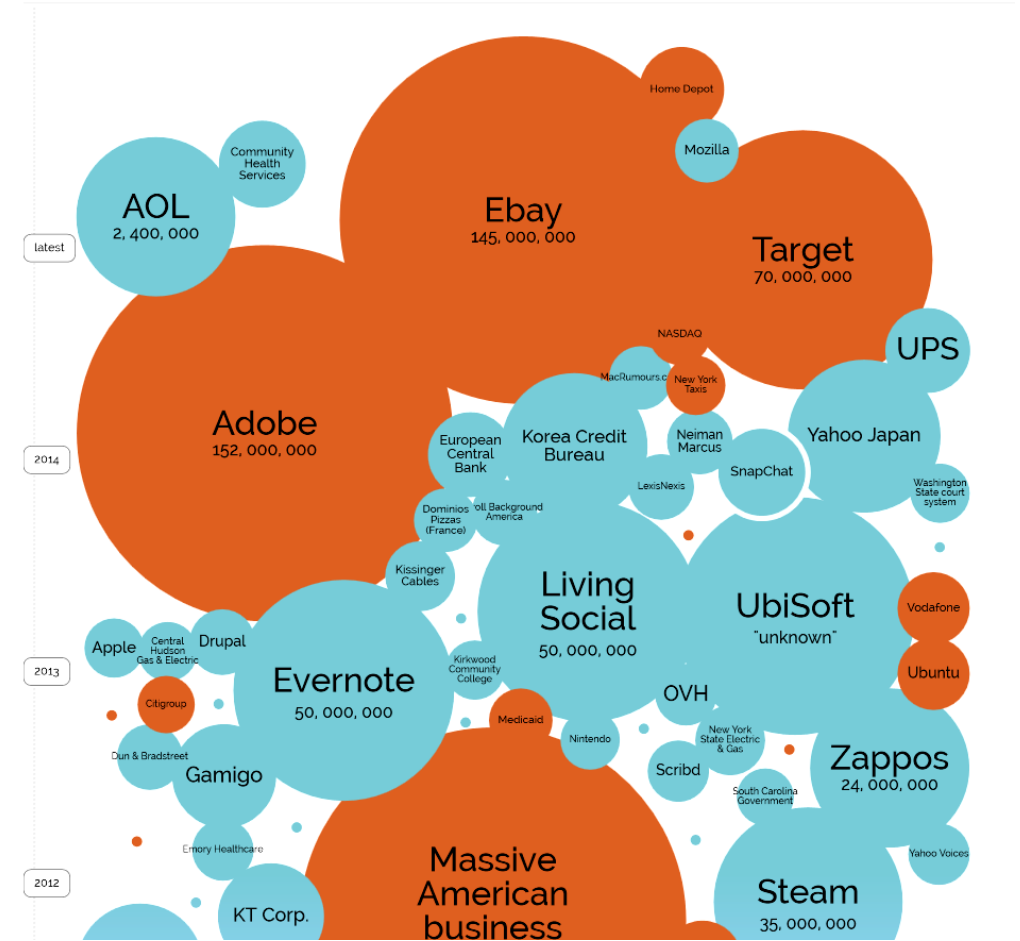
Increase of Cyber attacks



Adapt Security Policies



Unusable & Unsecure Password Policies



Infographic: Password Leaks, 2012-2014 - [\[Link\]](#)

# Literature Review

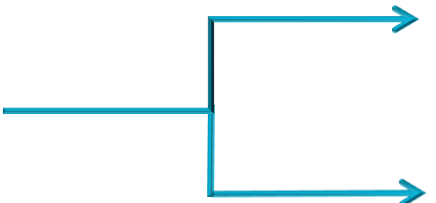
- Analysis of Passwords
- User Studies
- Password Policies Analysis

# Literature Review

- Analysis of Passwords
  - Password Strength
  - Number of Passwords & Reuse
- User Studies
- Password Policies Analysis

# Literature Review

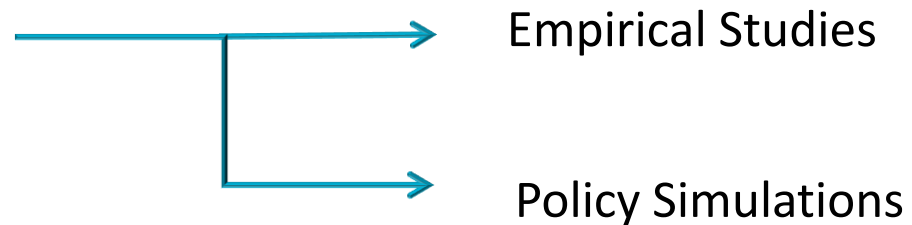
- Analysis of Passwords

- User Studies 
  - User Password Management
  - User Behavioural Models & Theories

- Password Policies Analysis

# Literature Review

- Analysis of Passwords
- User Studies
- Password Policies Analysis



# Methodology

- Review of Standards and Guidelines
- Qualitative Analysis

# Methodology

- Review of Standards and Guidelines :

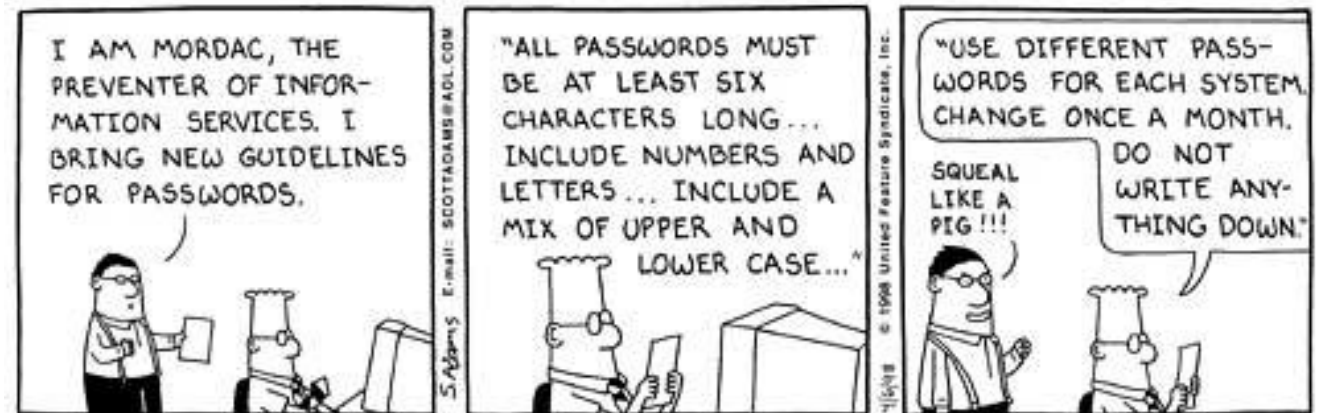


- 10 Candidates
- Qualitative Analysis :
  - Face-to-Face Interviews
  - Developers, Policy Makers & InfoSec Specialists

# Discussion of Results

- The Compliance Problem

- Lack of Practical Advice



*"Pictures as passwords", Belt Ibérica 2004 [\[Link\]](#)*

- Complex is Better

# Recommendations

- Increase communication between Researchers & Professionals
- Improve the Efficiency of User Training
- More Usable Oriented Standards & Guidelines

# Summary


- Contributions
- Limitations
- Future Work

# Summary

- Contributions
  - 1. Qualitative Analysis of Policy Makers
  - 2. A review of the current state of guidance
  - 3. Top 10 Advice for Developers
  - 4. Recommendations for Developers/Researchers/Auditors
- Limitations
- Future Work

# Summary

- Contributions

- Limitations 

```
graph LR; A[Limitations] --> B[Time Framework]; A --> C[Sample Size]
```

- Future Work

# Summary

- Contributions
- Limitations
- Future Work



# Thank You for Listening



This belief of the fundamental conflict between strong computer security mechanisms and usable computer... According to this belief a computer system must employ security mechanisms that are sophisticated and complex and therefore difficult to use. <sup>1</sup>



<sup>1</sup>Prof. Matt Bishop “Security and Usability: Designing Secure Systems that People Can Use” – p.1, Chapter I, Cranor (2005)